CHAPTER

2

UNDERSTANDING COMPUTER INVESTIGATIONS

After reading this chapter and completing the exercises, you will be able to:

- Explain how to prepare a computer investigation
- Apply a systematic approach to an investigation
- Describe procedures for corporate high-tech investigations
- Explain requirements for data recovery workstations and software
- Describe how to conduct an investigation
- Explain how to complete and critique a case

This chapter gives you an overview of how to manage a computing investigation. You learn about the problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider. This chapter introduces ProDiscover Basic, a GUI computer forensics tool. Throughout this chapter, you learn details about how other computer forensics tools are used in an investigation, too. You also explore standard problem-solving techniques.

As a basic computer user, you can solve most software problems by working with a GUI tool. A forensics professional, however, needs to interact with primary levels of the OS that are more fundamental than a GUI. Some computer forensics software tools involve working at the command line, and you should learn how to use these tools because in some cases, the command line is your only option. Appendix D includes examples of how to use DOS forensics tools.

In this chapter, you work with forensic disk images from small thumb drives to perform the activities and projects in this chapter. After you know how to search for and find data on a small storage device, you can apply the same techniques to a large disk, such as a 200 GB hard disk.

Preparing a Computer Investigation

Your role as a computer forensics professional is to gather evidence from a suspect's computer and determine whether the suspect committed a crime or violated a company policy. If the evidence suggests that a crime or policy violation has been committed, you begin to prepare a case, which is a collection of evidence you can offer in court or at a corporate inquiry. This process involves investigating the suspect's computer and then preserving the evidence on a different computer. Before you begin investigating, however, you must follow an accepted procedure to prepare a case. By approaching each case methodically, you can evaluate the evidence thoroughly and document the chain of evidence, or **chain of custody**, which is the route the evidence takes from the time you find it until the case is closed or goes to court.

The following sections present two sample cases—one involving a computer crime and another involving a company policy violation. Each example describes the typical steps of a forensics investigation, including gathering evidence, preparing a case, and preserving the evidence.

An Overview of a Computer Crime

Law enforcement officers often find computers and computer components as they're investigating crimes, gathering other evidence, or making arrests. Computers can contain information that helps law enforcement officers determine the chain of events leading to a crime or information that provides evidence that's more likely to lead to a conviction. As an example of a case in which computers were involved in a crime, the police raided a suspected drug dealer's home and found a computer, several floppy disks and thumb drives (also called keychain drives or memory sticks), a personal digital assistant (PDA), and a cell phone in a bedroom (see Figure 2-1). The computer was "bagged and tagged," meaning it was placed in evidence bags along with the storage media and then labeled with tags as part of the search and seizure.

The lead detective on the case wants you to investigate the computer to find and organize data that could be evidence of a crime, such as files containing names of the drug dealer's contacts. The acquisitions officer gives you documentation of items the investigating officers collected with the computer, including a list of other storage media, such as removable disks and CDs. The acquisitions officer also notes that the computer is a Windows XP system, and the machine was running when it was discovered. Before shutting down the computer, the acquisitions officer photographs all open windows on the Windows desktop, including one showing Windows Explorer, and gives you the photos.

As a computer forensics investigator, you're grateful the officers followed proper procedure when acquiring the evidence. With digital evidence, it's important to realize how easily key data, such as last access date, can be altered by an overeager investigator who's first on the scene. The U.S. Department of Justice (DOJ) has a document you can download that reviews proper acquisition of electronic evidence. The specific link for search and seizure of

Figure 2-1 The crime scene

computers is at *www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm*. Note that this link might change with newer updates. To locate the most current document at this Web site, use the search feature.

In your preliminary assessment, you assume that the hard disk and storage media include intact files, such as e-mail messages, deleted files, and hidden files. A range of software is available for use in your investigation; your office uses the tool Technology Pathways ProDiscover.

This chapter introduces you to the principles applied to computer forensics. In Chapter 7, you learn the strengths and weaknesses of several software packages.

Because some cases involve computers running legacy OSs, older versions of tools often need to be used in forensics investigations. For example, Norton DiskEdit is an older tool that was last available on the Norton SystemWorks 2000 CD.

After your preliminary assessment, you identify the potential challenges in this case. Because drug dealers don't usually make information about their accomplices available, the files on the disks you received are probably **password protected**. You might need to acquire **password-cracking software** or find an expert who can help you decrypt a file.

Later, you perform the steps needed to investigate the case, including how to address risks and obstacles. Then you can begin the actual investigation and data retrieval.

An Overview of a Company Policy Violation

Companies often establish policies for employee use of computers. Employees surfing the Internet, sending personal e-mail, or using company computers for personal tasks during work hours can waste company time. Because lost time can cost companies millions of dollars, computer forensics specialists are often used to investigate policy violations. The following example describes a company policy violation.

Manger Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked at the firm as an account representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area. Steve would like to know whether there's any information on George's computer and storage media that might offer a clue to George's whereabouts and job performance concerns. To help determine George and Martha's whereabouts, you must take a systematic approach, described in the following section, to examining and analyzing the data found on George's desk.

Taking a Systematic Approach

When preparing a case, you can apply standard systems analysis steps, explained in the following list, to problem solving. Later in this chapter, you apply these steps to cases.

- *Make an initial assessment about the type of case you're investigating*—To assess the type of case you're handling, talk to others involved in the case and ask questions about the incident. Have law enforcement or company security officers already seized the computer, disks, and other components? Do you need to visit an office or another locale? Was the computer used to commit a crime, or does it contain evidence about another crime?
- *Determine a preliminary design or approach to the case*—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or if you have to wait until evening or weekend hours. If you're preparing a criminal case, determine what information law enforcement officers have already gathered.
- *Create a detailed checklist*—Refine the general outline by creating a detailed checklist of steps to take and an estimated amount of time for each step. This outline helps you stay on track during the investigation.

- *Determine the resources you need*—Based on the OS of the computer you're investigating, list the software you plan to use for the investigation, noting any other software or tools you might need.
- *Obtain and copy an evidence disk drive*—In some cases, you might be seizing multiple computers along with Zip disks, Jaz drives, CDs, thumb drives, PDAs, and other removable media. (For the examples in this chapter, you're using only thumb drives.) Make a forensic copy of the disk.
- *Identify the risks*—List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.
- *Mitigate or minimize the risks*—Identify how you can minimize the risks. For example, if you're working with a computer on which the suspect has likely password-protected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.
- *Test the design*—Review the decisions you've made and the steps you've already completed. If you have already copied the original media, a standard part of testing the design involves comparing hash signatures (discussed in Chapters 4 and 5) to ensure that you made a proper copy of the original media.
- *Analyze and recover the digital evidence*—Using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence.
- *Investigate the data you recover*—View the information recovered from the disk, including existing files, deleted files, and e-mail, and organize the files to help prove the suspect's guilt or innocence.
- *Complete the case report*—Write a complete report detailing what you did and what you found.
- *Critique the case*—Self-evaluation is an essential part of professional growth. After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance.

The amount of time and effort you put into each step varies depending on the nature of the investigation. For example, in most casework, you need to create a simple investigation plan so that you don't overlook any steps. However, if a case involves many computers with complex issues to identify and examine, a detailed plan with periodic review and updates is essential. A systematic approach helps you discover the information you need for your case, and you should gather as much information as possible.

For all computing investigations, you must be prepared for the unexpected, so you should always have a contingency plan for the investigation. A contingency plan can consist of

anything to help you complete the investigation, from alternative software and hardware tools to other methods of approaching the investigation.

Assessing the Case

As mentioned, identifying case requirements involves determining the type of case you're investigating. Doing so means you should systematically outline the case details, including the nature of the case, the type of evidence available, and the location of the evidence.

In the company-policy violation case, suppose you have been asked to investigate George Montgomery. Steve Billings had the IT Department confiscate all of George's data storage media that might contain information about his whereabouts. After talking to George's co-workers, Steve learned that George has been conducting a personal business on the side using company computers. Therefore, the focus of the case has changed from a missing person to a possible employee abuse of corporate resources. You can begin assessing this case as follows:

- *Situation*—Employee abuse case.
- *Nature of the case*—Side business conducted on the employer's computer.
- *Specifics of the case*—The employee is reportedly conducting a side business on his employer's computer that involves registering domain names for clients and setting up their Web sites at local ISPs. Co-workers have complained that he's been spending too much time on his own business and not performing his assigned work duties. Company policy states that all company-owned computing assets are subject to inspection by company management at any time. Employees have no expectation of privacy when operating company computer systems.
- *Type of evidence*—USB thumb drive.
- *Operating system*—Microsoft Windows XP.
- *Known disk format*—FAT16.
- *Location of evidence*—One USB thumb drive recovered from the employee's assigned computer.

Based on these details, you can determine the case requirements. You now know that the nature of the case involves employee abuse of company assets, and you're looking for evidence that an employee was conducting his own business using his employer's computers. On the USB device retrieved from George's computer, you're looking for any information related to Web sites, ISPs, or domain names. You know that the computer OS is Windows XP, and the USB thumb drive uses the FAT16 file system. To duplicate the USB thumb drive and find deleted and hidden files, you need a reliable computer forensics tool. Because the USB thumb drive has already been retrieved, you don't need to obtain the drive yourself.

You call this case the Domain Name case and determine that your task is to gather data from the storage media seized to confirm or deny the allegation that George is conducting his own business on company time and computers. Remember that he's only suspected of asset

abuse, and the evidence you obtain might be exculpatory—meaning it could prove his innocence. You must always maintain an unbiased perspective and be objective in all your fact-findings. If you are systematic and thorough, you're more likely to produce consistently reliable results.

Planning Your Investigation

Now that you have identified the requirements of the Domain Name case, you can plan your investigation. You have already determined the kind of evidence you need; now you can identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis. These steps become the basic plan for your investigation and indicate what you should do and when. To investigate the Domain Name case, you should perform the following general steps. Most of these steps are explained in more detail in the following sections.

1. Acquire the USB thumb drive from George's manager.
2. Complete an evidence form and establish a chain of custody.
3. Transport the evidence to your computer forensics lab.
4. Secure the evidence in an **approved secure container**.
5. Prepare your forensic workstation.
6. Obtain the evidence from the secure evidence container.
7. Make a forensic copy of the evidence drive (in this case, the USB thumb drive).
8. Return the evidence drive to the secure evidence container.
9. Process the copied evidence drive with your computer forensics tools.

The approved secure container you need in Step 4 should be a locked, fireproof locker or cabinet that has limited access. Limited access means that only you and other authorized personnel can open the evidence container.

The first rule for all investigations is to preserve the evidence, which means it should not be tampered with or contaminated. Because the IT Department staff confiscated the storage media, you need to go to them for the evidence. The IT Department manager confirms that the storage media has been locked in a secure cabinet since it was retrieved from George's desk. Keep in mind that even though this case is a corporate policy matter, many cases are thrown out because the chain of custody can't be proved or has been broken. When this happens, there's the possibility that the evidence has been compromised.

To document the evidence, you record details about the media, including who recovered the evidence and when and who possessed it and when. Use an **evidence custody form**, also

called a chain-of-evidence form, which helps you document what has and has not been done with the original evidence and forensic copies of the evidence.

Depending on whether you're working in law enforcement or private corporate security, you can create an evidence custody form to fit your environment. This form should be easy to read and use. It can contain information for one or several pieces of evidence. Consider creating a **single-evidence form** (which lists each piece of evidence on a separate page) and a **multi-evidence form** (see Figure 2-2), depending on the administrative needs of your investigation.

If necessary, document how to use your evidence custody form. Clear instructions help users remain consistent when completing the form and ensure that everyone uses the same definitions for collected items. Standardization helps maintain consistent quality for all investigations and avoid confusion and mistakes about the evidence you collect.

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 2-2 A sample multi-evidence form used in a corporate environment

An evidence custody form usually contains the following information:

- *Case number*—The number your organization assigns when an investigation is initiated.
- *Investigating organization*—The name of your organization. In large corporations with global facilities, several organizations might be conducting investigations in different geographic areas.
- *Investigator*—The name of the investigator assigned to the case. If many investigators are assigned, insert the lead investigator's name.
- *Nature of case*—A short description of the case. For example, in the corporate environment, it might be "Data recovery for corporate litigation" or "Employee policy violation case."
- *Location evidence was obtained*—The exact location where the evidence was collected. If you're using multi-evidence forms, a new form should be created for each location.
- *Description of evidence*—Describes the evidence, such as "hard disk drive, 20 GB" or "one USB thumb drive, 128 MB." On a multi-evidence form, write a description for each item of evidence you acquire.
- *Vendor name*—The name of the manufacturer of the computer evidence. List a 20 GB hard drive, for example, as a Maxtor 20 GB hard drive, or describe a USB thumb drive as an Attache 1 GB PNY Technologies drive. In later chapters, you see how differences among manufacturers can affect data recovery.
- *Model number or serial number*—List the model number or serial number (if available) of the computer component. Many computer components, including hard drives, memory chips, and expansion slot cards, have model numbers but not serial numbers.
- *Evidence recovered by*—The name of the investigator who recovered the evidence. The chain of custody for evidence starts with this information. If you insert your name, for example, you're declaring that you have taken control of the evidence. It's now your responsibility to ensure that nothing damages the evidence and no one tampers with it. The person placing his or her name on this line is responsible for preserving, transporting, and securing the evidence.
- *Date and time*—The date and time the evidence was taken into custody. This information establishes exactly when the chain of custody starts.
- *Evidence placed in locker*—Indicates which approved secure container is used to store evidence and when the evidence was placed in the container.

- *Item #/Evidence processed by/Disposition of evidence/Date/Time*—When you or another authorized investigator obtains evidence from the evidence locker for processing and analysis, list the item number and your name, and then describe what was done to the evidence.
- *Page*—The forms used to catalog all evidence for each location should have page numbers. List the page number, and indicate the total number of pages for this group of evidence. For example, if you collected 15 pieces of evidence at one location and your form has only 10 lines, you need to fill out two multi-evidence forms. The first form is filled in as "Page 1 of 2," and the second page is filled in as "Page 2 of 2."

Figure 2-3 shows a single-evidence form, which lists only one piece of evidence per page. This form gives you more flexibility in tracking separate pieces of evidence for your chain-of-custody log. It also has more space for descriptions, which is helpful when finalizing the investigation and creating a case report. With this form, you can accurately account for what was done to the evidence and what was found. Use evidence forms as a reference to all actions taken for your investigative analysis.

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of ___

Figure 2-3 A single-evidence form

You can use both multi-evidence and single-evidence forms in your investigation. By using two forms, you can keep the single-evidence form with the evidence and the multi-evidence form in your report file. Two forms also provide redundancy that can be used as a quality control for your evidence.

Securing Your Evidence

Computing investigations demand that you adjust your procedures to suit the case. For example, if the evidence for a case includes an entire computer system and associated storage media, such as floppy disks, Zip and Jaz cartridges, 4 mm DDS digital audio tape (DAT), and USB thumb drives, you must be flexible when you account for all the items. Some evidence is small enough to fit into an evidence bag. Other items, such as the CPU cabinet, monitor, keyboard, and printer, are too large.

To secure and catalog the evidence contained in large computer components, you can use large **evidence bags**, tape, tags, labels, and other products available from police supply vendors or office supply stores. When gathering products to secure your computer evidence, make sure they are safe and effective to use on computer components. Be cautious when handling any computer component to avoid damaging the component or coming into contact with static electricity, which can destroy digital data. For this reason, make sure you use antistatic bags when collecting computer evidence. Consider using an antistatic pad with an attached wrist strap, too. Both help prevent damage to computer evidence.

Be sure to place computer evidence in a well-padded container. Padding prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab. Save discarded hard drive boxes, antistatic bags, and packing material for computer hardware when you or others acquire computer devices.

Because you might not have everything necessary to secure your evidence, you have to improvise. Securing evidence often requires you to build secure containers. If the computer component is large and contained in its own casing, such as a CPU cabinet, you can use evidence tape to seal all openings on the cabinet. Placing evidence tape over drive bays, insertion slots for power supply cords and USB cables, and any other openings ensures the security of evidence. As a standard practice, you should write your initials on the tape before applying it to the evidence. This practice makes it possible to prove later in court that the evidence hasn't been tampered with because the case could not have been opened nor could power have been supplied to the closed case with this tape in place. If the tape had been replaced, your initials wouldn't be present, which would indicate tampering. If you transport a CPU case, place new disks in the floppy disk drives to reduce possible drive damage while you're moving the computer.

Computer components require specific temperature and humidity ranges. If it's too cold, hot, or wet, computer components and magnetic media can be damaged. Even heated car seats can damage digital media, and placing a computer on top of a two-way car radio in the

trunk can damage magnetic media. When collecting computer evidence, make sure you have a safe environment for transporting and storing it until a secure evidence container is available.

Procedures for Corporate High-Tech Investigations

As an investigator, you need to develop formal procedures and informal checklists to cover all issues important to high-tech investigations. These procedures are necessary to ensure that correct techniques are used in an investigation. Use informal checklists to be certain that all evidence is collected and processed properly. This section lists some sample procedures that computing investigators commonly use in corporate high-tech investigations.

Employee Termination Cases

The majority of investigative work for termination cases involves employee abuse of corporate assets. Incidents that create a hostile work environment, such as viewing pornography in the workplace and sending inappropriate e-mail messages, are the predominant types of cases investigated. The following sections describe key points for conducting an investigation that might lead to an employee's termination. Consulting with your organization's general counsel and Human Resources Department for specific directions on how to handle these investigations is recommended. Your organization must have appropriate policies in place, as described in Chapter 1.

Internet Abuse Investigations

The information in this section applies to an organization's internal private networks, not a public ISP. Consult with your organization's general counsel after reviewing this list, and make changes according to their directions to build your own procedures. To conduct an investigation involving Internet abuse, you need the following:

- The organization's Internet proxy server logs
- Suspect computer's IP address obtained from your organization's network administrator
- Suspect computer's disk drive
- Your preferred computer forensics analysis tool (ProDiscover, FTK, EnCase, X-Ways Forensics, and so forth)

The following steps outline the recommended processing of an Internet abuse case:

1. Use the standard forensic analysis techniques and procedures described in this book for the disk drive examination.
2. Using tools such as DataLifter or Forensic Toolkit's Internet keyword search option, extract all Web page URL information.

3. Contact the network firewall administrator and request a proxy server log, if it's available, of the suspect computer's network device name or IP address for the dates of interest. Consult with your organization's network administrator to confirm that these logs are maintained and how long the time to live (TTL) is set for the network's IP address assignments that use Dynamic Host Configuration Protocol (DHCP).
4. Compare the data recovered from forensic analysis to the proxy server log data to confirm that they match.
5. If the URL data matches the proxy server log and the forensic disk examination, continue analyzing the suspect computer's disk drive data, and collect any relevant downloaded inappropriate pictures or Web pages that support the allegation. If there are no matches between the proxy server logs, and the forensic examination shows no contributing evidence, report that the allegation is unsubstantiated.

NOTE

Before investigating an Internet abuse case, research your state or country's privacy laws. Many countries have unique privacy laws that restrict the use of computer log data, such as proxy server logs or disk drive cache files, for any type of investigation. Some state or federal laws might supersede your organization's employee policies. Always consult with your organization's attorney. For companies with international business operations, jurisdiction is a problem; what is legal in the United States, such as examining and investigating a proxy server log, might not be legal in Germany, for example.

For investigations in which the proxy server log doesn't match the forensic analysis that found inappropriate data, continue the examination of the suspect computer's disk drive. Determine when inappropriate data was downloaded to the computer and whether it was through an organization's intranet connection to the Internet. Employees might have used their employer's laptop computers to connect to their own ISPs to download inappropriate Web content. For these situations, you need to consult your organization's employee policy guidelines for what's considered appropriate use of the organization's computing assets.

E-mail Abuse Investigations

E-mail investigations typically include spam, inappropriate and offensive message content, and harassment or threats. E-mail is subject to the same restrictions as other computer evidence data, in that an organization must have a properly defined policy as described in Chapter 1. The following list is what you need for an investigation involving e-mail abuse:

- An electronic copy of the offending e-mail that contains message header data; consult with your e-mail server administrator
- If available, e-mail server log records; consult with your e-mail server administrator to see whether they are available

- For e-mail systems that store users' messages on a central server, access to the server; consult with your e-mail server administrator
- For e-mail systems that store users' messages on a computer as an Outlook .pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it
- Your preferred computer forensics analysis tool, such as Forensic Toolkit or ProDiscover

This is the recommended procedure for e-mail investigations:

1. For computer-based e-mail data files, such as Outlook .pst or .ost files, use the standard forensic analysis techniques and procedures described in this book for the disk drive examination.
2. For server-based e-mail data files, contact the e-mail server administrator and obtain an electronic copy of the suspect and victim's e-mail folder or data.
3. For Web-based e-mail investigations, such as Hotmail or Yahoo! mail, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information.
4. Examine header data of all messages of interest to the investigation.

Attorney-Client Privilege Investigations

When conducting a computer forensics analysis under **attorney-client privilege (ACP)** rules for an attorney, you must keep all findings confidential. The attorney you're working for is the ultimate authority over the investigation. For investigations of this nature, attorneys typically request that you extract all data from disk drives. It's your responsibility to comply with the attorney's directions. Because of the large quantities of data a disk drive can contain, the attorney will want to know about everything on the drives of interest.

Many attorneys like to have printouts of the data you have recovered, but printouts can present problems when you have log files with several thousand pages of data or CAD drawing programs that can be read only by proprietary programs. You need to persuade and educate many attorneys on how digital evidence can be viewed electronically. In addition, learn how to teach attorneys and paralegals to sort through data files so that you can help them efficiently analyze the huge amount of data a forensic examination produces.

You can also encounter problems if you find data in the form of binary files, such as CAD drawings. Examining these types of files requires using the CAD program that created them. In addition, engineering companies often have specialized drafting programs. Discovery demands for lawsuits involving a product that caused injury or death requires extracting design plans for attorneys and expert witnesses to review. You will be responsible for locating the programs for these design plans so that attorneys and expert witnesses can view the evidence files.

The following list shows the basic steps for conducting an ACP case:

1. Request a memorandum from the attorney directing you to start the investigation. The memorandum must state that the investigation is privileged communication and list your name and any other associates' names assigned to the case.
2. Request a list of keywords of interest to the investigation.
3. When you have received the memorandum, initiate the investigation and analysis. Any findings you made before receiving the memorandum are subject to discovery by the opposing attorney.
4. For disk drive examinations, make two bit-stream images (discussed later in this chapter) of the disk using a different tool for each image, such as EnCase for the first and ProDiscover or SafeBack for the second. If you have large enough storage drives, make each bit-stream image uncompressed to ensure that if it becomes corrupt, you can still examine uncorrupted areas with your preferred forensic analysis tool.
5. If possible, compare hash signatures on all files on the original and re-created disks. Typically, attorneys want to view all data, even if it's not relevant to the case. Many GUI forensics tools perform this task during bit-stream imaging of the disk drive.
6. Methodically examine every portion of the disk drive (both allocated and unallocated data areas) and extract all data.
7. Run keyword searches on allocated and unallocated disk space. Follow up the search results to determine whether the search results contain information that supports the case.
8. For Windows OSs, use specialty tools to analyze and extract data from the Registry, such as AccessData Registry Viewer or a Registry viewer program (discussed in more detail in Chapter 6). Use the Edit, Find menu option in the Registry Editor, for example, to search for keywords of interest to the investigation.
9. For binary data files such as CAD drawings, locate the correct software product and, if possible, make printouts of the binary file content. If the data files are too large, load the specialty application on a separate workstation with the recovered binary files so that the attorney can view them.
10. For unallocated data (file slack space or free space, explained in Chapter 6) recovery, use a tool that removes or replaces nonprintable data, such as X-Ways Forensics Specialist Gather Text function.
11. Consolidate all recovered data from the evidence bit-stream image into well-organized folders and subfolders. Store the recovered data output using a logical and easy-to-follow storage method for the attorney or paralegal.

Here are some other guidelines to remember for ACP cases:

- Minimize all written communications with the attorney; use the telephone when you need to ask questions or provide information related to the case.
- Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product" as defined under the attorney-work-product rule.
- Assist the attorney and paralegal in analyzing the data.

If you have difficulty complying with the directions or don't understand the directives from the memorandum, contact the attorney and explain the problem. Always keep an open line of verbal communication with the attorney during these types of investigations. If you're communicating via e-mail, use encryption such as PGP or another security e-mail service for all messages.

Media Leak Investigations

In the corporate environment, controlling sensitive data can be difficult. Disgruntled employees, for example, might send an organization's sensitive data to a news reporter. The reasons for media leaks range from employees' efforts to embarrass management to a rival conducting a power struggle between competing internal organizations. Another concern is the premature release of information about new products, which can disrupt operations and cause market share loss for a business if it's made public too soon. Media leak investigations can be time consuming and resource intensive. Because management wants to find who leaked information, scope creep during the investigation is not uncommon.

Consider the following for media leak investigations:

- Examine e-mail, both the organization's e-mail servers and private e-mail accounts (Hotmail, Yahoo!, Gmail, and so on), on company-owned computers.
- Examine Internet message boards (such as Yahoo!); research the Internet for any information about the company or product. Use Internet search engines to run word searches related to the company, product, or leaked information. For example, you might search for "graphite-composite bicycle sprocket" for a bicycle manufacturer that was the victim of a media leak about a new product in development.
- Examine proxy server logs to check for log activities that might show use of free e-mail services, such as Hotmail, Yahoo!, or Gmail. Track back to the specific workstation where these messages originated and perform a forensic analysis on the disk drives to help determine what was communicated.
- Examine known suspects' workstations, perform computer forensics examinations on persons of interest, and develop other leads on possible associates.
- Examine all company telephone records for any calls to known media organizations.

The following list outlines steps to take for media leaks:

1. Interview management privately to get a list of employees who have direct knowledge of the sensitive data.
2. Identify the media source that published the information.
3. Review company phone records to see who might have had contact with the news service.
4. Obtain a listing of keywords related to the media leak.
5. Perform keyword searches on proxy and e-mail servers.
6. Discreetly conduct forensic disk acquisitions and analysis of employees of interest.
7. From the forensic disk examinations, analyze all e-mail correspondence and trace any sensitive messages to other people who haven't been listed as having direct knowledge of the sensitive data.
8. Expand the discreet forensic disk acquisition and analysis for any new persons of interest.
9. Consolidate and review your findings periodically to see whether new clues can be discovered.
10. Routinely report findings to management and discuss how much further to continue the investigation.

Industrial Espionage Investigations

Industrial espionage cases, similar to media leaks, can be time consuming and are subject to the same scope creep problems. This section offers some guidelines on how to deal with industrial espionage investigations. Be aware that cases dealing with foreign nationals might be violations of the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). For more information on ITAR, see the U.S. Department of State's Web site (*www.state.gov*; substitute the actual state name for *state*) or do an Internet search for "International Traffic in Arms Regulations." For EAR information, see the U.S. Department of Commerce Web site (*www.doc.gov*) or do an Internet search for "Export Administration Regulations."

Unlike the other corporate investigations covered in this section, all suspected industrial espionage cases should be treated as criminal investigations. The techniques described here are for the private network environment and internal investigations that haven't yet been reported to law enforcement officials. Make sure you don't become an agent of law enforcement by filing a complaint of a suspected espionage case before substantiating the

allegation. The following list includes staff you might need when planning an industrial espionage investigation. This list isn't exhaustive, so be creative and apply your talents to improve on these recommendations.

- The computing investigator who is responsible for disk forensic examinations
- The technology specialist who is knowledgeable of the suspected compromised technical data
- The network specialist who can perform log analysis and set up network sniffers to trap network communications of possible suspects
- The threat assessment specialist (typically an attorney) who is familiar with federal and state laws and regulations related to ITAR or EAR and industrial espionage

In addition, consider the following guidelines when initiating an international espionage investigation:

- Determine whether this investigation involves a possible industrial espionage incident, and then determine whether it falls under ITAR or EAR.
- Consult with corporate attorneys and upper management if the investigations must be conducted discreetly.
- Determine what information is needed to substantiate the allegation of industrial espionage.
- Generate a list of keywords for disk forensics and sniffer monitoring.
- List and collect resources needed for the investigation.
- Determine the goal and scope of the investigation; consult with management and the company's attorneys on how much work you should do.
- Initiate the investigation after approval from management, and make regular reports of your activities and findings.

The following are planning considerations for industrial espionage investigations:

- Examine all e-mail of suspected employees, both company-provided e-mail and free Web-based services.
- Search Internet newsgroups or message boards for any postings related to the incident.
- Initiate physical surveillance with cameras on people or things of interest to the investigation.
- If available, examine all facility physical access logs for sensitive areas, which might include secure areas where smart badges or video surveillance recordings are used.
- If there's a suspect, determine his or her location in relation to the vulnerable asset that was compromised.
- Study the suspect's work habits.
- Collect all incoming and outgoing phone logs to see whether any unique or unusual places were called.

When conducting an industrial espionage case, follow these basic steps:

1. Gather all personnel assigned to the investigation and brief them on the plan and any concerns.
2. Gather the resources needed to conduct the investigation.
3. Start the investigation by placing surveillance systems, such as cameras and network sniffers, at key locations.
4. Discreetly gather any additional evidence, such as the suspect's computer disk drive, and make a bit-stream image for follow-up examination.
5. Collect all log data from networks and e-mail servers, and examine them for unique items that might relate to the investigation.
6. Report regularly to management and corporate attorneys on your investigation's status and current findings.
7. Review the investigation's scope with management and corporate attorneys to determine whether it needs to be expanded and more resources added.

Interviews and Interrogations in High-Tech Investigations

Becoming a skilled interviewer and interrogator can take many years of experience. Typically, a corporate computing investigator is a technical person acquiring the evidence for an investigation. Many large organizations have full-time security investigators with years of training and experience in criminal and civil investigations and interviewing techniques. Few of these investigators have any computing or network technical skills, so you might be asked to assist in interviewing or interrogating a suspect when you have performed a forensic disk analysis on that suspect's machine.

An interrogation is different from an interview. An **interview** is usually conducted to collect information from a witness or suspect about specific facts related to an investigation. An **interrogation** is the process of trying to get a suspect to confess to a specific incident or crime. An investigator might change from an interview to an interrogation when talking to a witness or suspect. The more experience and training investigators have in the art of interviewing and interrogating, the more easily they can determine whether a witness is credible and possibly a suspect.

Your role as a computing investigator is to instruct the investigator conducting the interview on what questions to ask and what the answers should be. As you build rapport with the investigator, he or she might ask you to question the suspect. Watching a skilled interrogator is a learning experience in human relations skills.

If you're asked to assist in an interview or interrogation, prepare yourself by answering the following questions:

- What questions do I need to ask the suspect to get the vital information about the case?
- Do I know what I'm talking about, or will I have to research the topic or technology related to the investigation?
- Do I need additional questions to cover other indirect issues related to the investigation?

Common interview and interrogation errors include being unprepared for the interview or interrogation and not having the right questions or enough questions to increase your depth of knowledge. Make sure you don't run out of conversation topics; you need to keep the conversation friendly to gain the suspect's confidence. Avoid doubting your own skills, which might show the suspect you lack confidence in your ability.

Ingredients for a successful interview or interrogation require the following:

- Being patient throughout the session
- Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
- Being tenacious

Understanding Data Recovery Workstations and Software

Now you know what's involved in acquiring and documenting evidence. In Chapter 3, you examine a complete setup of a computer forensics lab, which is where you conduct your investigations and where most of your equipment and software are located, including secure evidence containers. Be aware that some companies that perform computer investigations also do data recovery, which is the more well-known and lucrative side of the business.

Remember the difference between data recovery and computer forensics. In data recovery, you don't necessarily need a sterile target drive when restoring the forensic image. Typically, the customer or your company just wants the data back. The other key difference is that in data recovery, you usually know what you're trying to retrieve. In computer forensics, you might have an idea of what you're searching for, but not necessarily.

To conduct your investigation and analysis, you must have a specially configured PC known as a **computer forensics workstation** (or "forensic workstation"), which is a computer

loaded with additional bays and forensics software. Depending on your needs, most computer forensics work can be performed on the following Microsoft OSs:

- MS-DOS 6.22
- Windows 95, 98, or Me
- Windows NT 3.5 or 4.0
- Windows 2000
- Windows XP
- Windows Vista

Chapters 3 and 7 cover the software resources you need and the forensics lab and workstation in detail. Visit *www.digitalintel.com* to examine the specifications of the Forensic Recovery of Evidence Device (F.R.E.D.) unit or *www.forensicpc.com* to examine the ForensicPC Dual Xeon Workstation and other current products.

In addition to the Windows OSs listed, you can use Linux or UNIX to conduct your analysis. Several open-source and freeware tools are available for this purpose. Windows server software, such as Windows Server 2003, isn't generally used for forensics work, although this might change because of memory and I/O conflicts with higher-end computer forensics applications.

If you start Windows while you're examining a hard disk, Windows alters the evidence disk by writing data to the Recycle Bin and corrupts the quality and integrity of the evidence you're trying to preserve. Chapter 6 covers which files Windows updates automatically at startup. Windows XP and 2000 systems also record the serial numbers of hard drives and CPUs in a file, which can be difficult to recover.

Of all the Microsoft OSs, the least intrusive (in terms of changing data) to disks is MS-DOS 6.22. With the continued evolution of Microsoft OSs, it's not always practical to use older MS-DOS platforms, however. Newer file system formats, such as NTFS, are accessible—that is, readable—only from Window NT or newer OSs. You can use one of several write-blockers that enable you to boot to Windows without writing any data to the evidence drive. In Chapter 4, you learn more about write-blockers and some inexpensive alternatives for preserving data during an acquisition.

There are many hardware write-blockers on the market. Some are inserted between the disk controller and the hard disk; others connect to USB or FireWire ports. Several vendors sell write-blockers, including Technology Pathways NoWrite FPU; Digital Intelligence UltraKit, UltraBlock, FireFly, FireChief 800, and USB Write Blocker; WiebeTECH Forensic DriveDock; Guidance Software FastBloc2; Paralan's SCSI Write Blockers; and Intelligent Computer Solutions (*www.ics-iq.com*) Image LinkMaSSter Forensics Hard Case.

Many older computer forensics acquisition tools work in the MS-DOS environment. These tools can operate from an MS-DOS window in Windows 98 or from the command prompt in Windows 2000/XP/Vista. Some of their functions are disabled or generate error messages when run from these OSs, however.

Windows products are being developed that make performing disk forensics easier. However, because Windows has limitations in performing disk forensics, you might need to develop skills in acquiring data with MS-DOS and Linux. In later chapters, you learn more about using these other tools. No single computer forensics tool can recover everything. Each tool and OS has its own strengths and weaknesses. Develop skills with as many tools as possible to become an effective computing investigator. Appendix D has additional information on how to use MS-DOS for data acquisitions.

Setting Up Your Workstation for Computer Forensics

With current computer forensics hardware and software, configuring a computer workstation or laptop as a forensic workstation is simple. All that's required are the following:

- A workstation running Windows XP or Vista
- A write-blocker device
- Computer forensics acquisition tool
- Computer forensics analysis tool
- A target drive to receive the source or suspect disk data
- Spare PATA or SATA ports
- USB ports

Additional useful items include the following:

- Network interface card (NIC)
- Extra USB ports
- FireWire 400/800 ports
- SCSI card
- Disk editor tool
- Text editor tool
- Graphics viewer program
- Other specialized viewing tools

In Chapter 3, you learn more about setting up and configuring a computer to be a forensic workstation.

Conducting an Investigation

Now you're ready to return to the Domain Name case. You have created a plan for the investigation, set up your forensic workstation, and installed the necessary forensic analysis software you need to examine the evidence. The type of software to install includes your preferred analysis tool, such as ProDiscover, EnCase, FTK, or X-Ways Forensics; an office suite, such as OpenOffice; and a graphics viewer, such as IrfanView. To begin conducting an investigation, you start by copying the evidence using a variety of methods. No single method retrieves all data from a disk, so using several tools to retrieve and analyze data is a good idea.

Start by gathering the resources you identified in your investigation plan. You need the following items:

- Original storage media
- Evidence custody form
- Evidence container for the storage media, such as an evidence bag
- Bit-stream imaging tool; in this case, the ProDiscover Basic acquisition utility
- Forensic workstation to copy and examine your evidence
- Securable evidence locker, cabinet, or safe

Gathering the Evidence

Now you're ready to gather evidence for the Domain Name case. Remember, you need antistatic bags and pads with wrist straps to prevent static electricity from damaging digital evidence. To acquire George Montgomery's storage media from the IT Department and then secure the evidence, you perform the following steps:

1. Arrange to meet the IT manager to interview him and pick up the storage media.
2. After interviewing the IT manager, fill out the evidence form, have him sign it, and then sign it yourself.
3. Store the storage media in an evidence bag, and then transport it to your forensic facility.
4. Carry the evidence to a secure container, such as a locker, cabinet, or safe.
5. Complete the evidence custody form. As mentioned, if you're using a multi-evidence form, you can store the form in the file folder for the case. If you're also using single-evidence forms, store them in the secure container with the evidence. Reduce the risk of tampering by limiting access to the forms.
6. Secure your evidence by locking the container.

Understanding Bit-stream Copies

A **bit-stream copy** is a bit-by-bit copy (also known as a sector copy) of the original drive or storage medium and is an exact duplicate. The more exact the copy, the better chance you have of retrieving the evidence you need from the disk. This process is usually referred to as "acquiring an image" or "making an image" of a suspect drive. A bit-stream copy is different from a simple backup copy of a disk. Backup software can only copy or compress files that are stored in a folder or are of a known file type. Backup software can't copy deleted files or e-mails or recover file fragments.

A **bit-stream image** is the file containing the bit-stream copy of all data on a disk or disk partition. For simplicity, it's usually referred to as an "image," "image save," or "image file." Some manufacturers also refer to it as a **forensic copy**. To create an exact image of an evidence disk, copying the image to a target disk that's identical to the evidence disk is preferable (see Figure 2-4). The target disk's manufacturer and model, in general, should be the same as the original disk's manufacturer and model. If the target disk is identical to the original, the size in bytes and sectors of both disks should also be the same. Some software tools that acquire images can accommodate a target disk that's a different size than the original. These imaging tools are discussed in Chapter 4. Older computer forensics tools designed for MS-DOS work only on a copied disk. Current GUI tools can work on both a disk drive and copied data sets that many manufacturers refer to as "image saves."

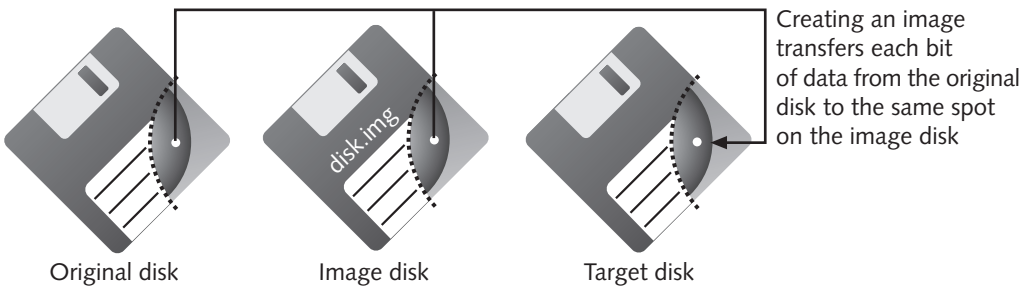

Creating an image transfers each bit of data from the original disk to the same spot on the image disk
disk.img
Original disk
Image disk
Target disk

Figure 2-4 Transfer of data from original to image to target

Occasionally, the track and sector maps on the original and target disks don't match, even if you use disks of exactly the same size that are different makes or models. Tools such as Guidance EnCase, NTI SafeBack, and DataArrest SnapCopy adjust for the target drive's geometry. Two other tools, X-Ways WinHex Specialist Edition and Technology Pathways ProDiscover, can copy sector by sector to equal-sized or larger disks without needing to force changes in the target disk's geometry.

Acquiring an Image of Evidence Media

After you retrieve and secure the evidence, you're ready to copy the evidence media and analyze the data. The first rule of computer forensics is to preserve the original evidence.

Then conduct your analysis only on a copy of the data—the image of the original medium. Several vendors provide MS-DOS, Linux, and Windows-based acquisition tools. Windows tools, however, require a write-blocking device when acquiring data from FAT or NTFS file systems. (Write-blockers are discussed in Chapter 4.)

Using ProDiscover Basic to Acquire a Thumb Drive

ProDiscover Basic from Technology Pathways is a forensics data analysis tool. You can use it to acquire and analyze data from several different file systems, such as Microsoft FAT and NTFS, Linux Ext2 and Ext3, and other UNIX file systems.

The DVD accompanying this book includes ProDiscover Basic. The installation program includes a user manual, ProDiscoverManual.pdf, in the C:\Program Files\Technology Pathways\ProDiscover folder (if the installation defaults are used). Read the user manual for instructions on installing it on your computer before you perform the following activity.

Before starting this activity, you need to create a work folder on your computer for data storage and other related files ProDiscover creates when acquiring and analyzing evidence. You can use any location and name for your work folder, but you'll see it referred to in activities as C:*Work* or simply "your work folder." To keep your files organized, you should also create subfolders for each chapter. For this chapter, create a *Work*\Chap02\Chapter folder to store files from in-chapter activities. Note that you might see work folder pathnames in screenshots that are slightly different from your own pathname.

The following steps show how to acquire an image of a thumb drive, but you can apply them to other media, such as disk drives and floppy disks. You can use any thumb drive already containing files to see how ProDiscover acquires data. To perform an acquisition on a USB thumb drive with ProDiscover Basic, follow these steps:

1. First, on the thumb drive, locate the write-protect switch (if one is available) and place the drive in write-protect mode. Now connect the thumb drive to your computer.

This activity is meant to introduce you to the ProDiscover Basic tool. Proper forensics processes require write-protecting any evidence media to ensure that it's not altered. In Chapter 4, you learn how to use hardware and software write-blocking methods.

2. To start ProDiscover Basic, click **Start**, point to **All Programs**, point to **ProDiscover**, and click **ProDiscover Basic**. If the Launch Dialog dialog box opens (see Figure 2-5), click **Cancel**.

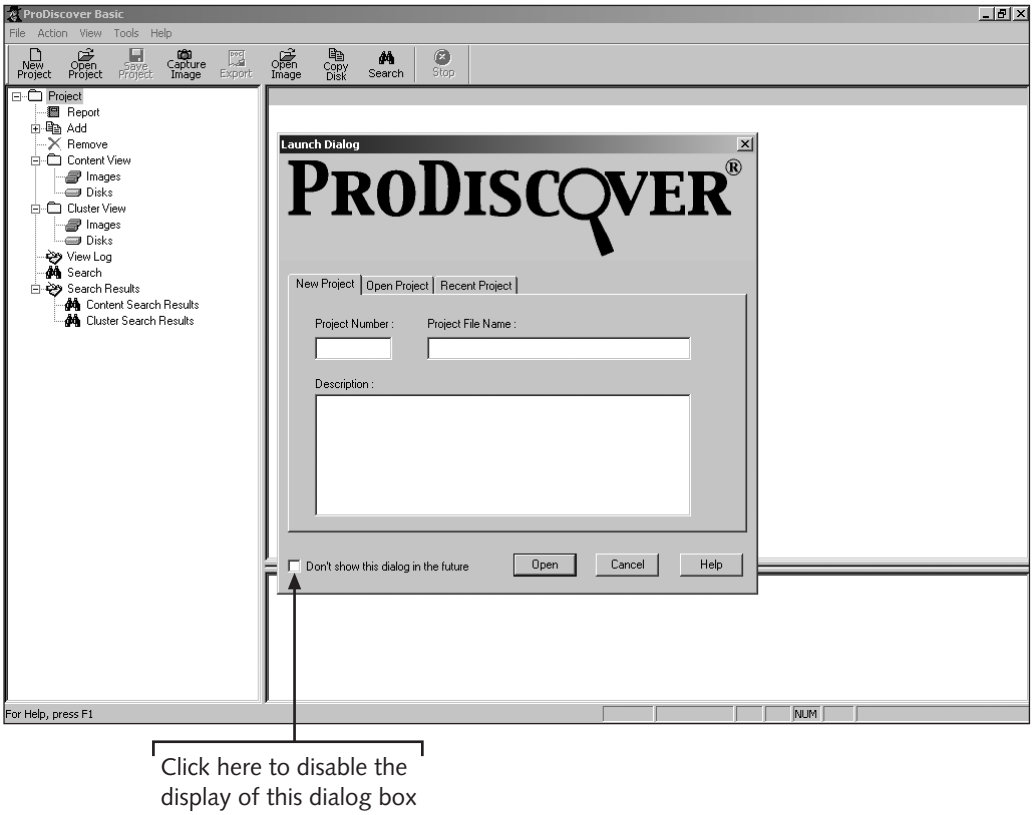


Figure 2-5 The main window in ProDiscover

For convenience, you can disable the display of this dialog box by clicking the check box indicated in Figure 2-5.

3. In the main window, click **Action**, **Capture Image** from the menu.
4. In the Capture Image dialog box shown in Figure 2-6, click the **Source Drive** drop-down list, and select the thumb drive.
5. Click the **>>** button next to the Destination text box. When the Save As dialog box opens, navigate to your work folder and enter a name for the image you're making, such as **InChp-prac** (see Figure 2-7). Click **Save** to save the file.

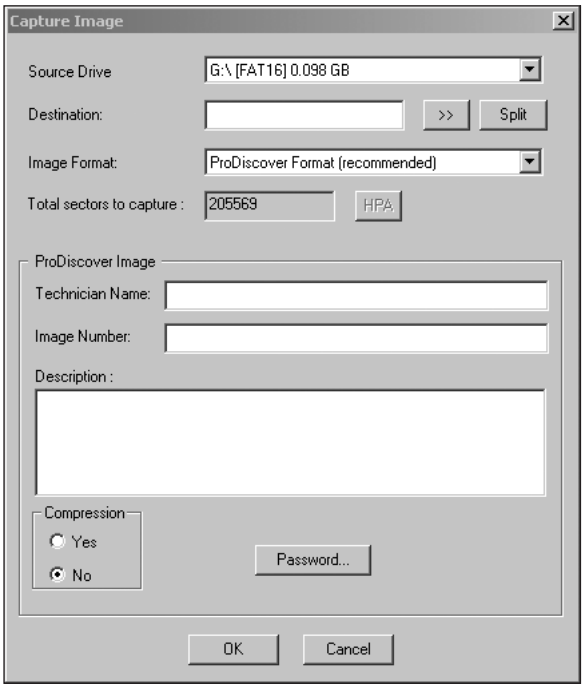


Figure 2-6 The Capture Image dialog box

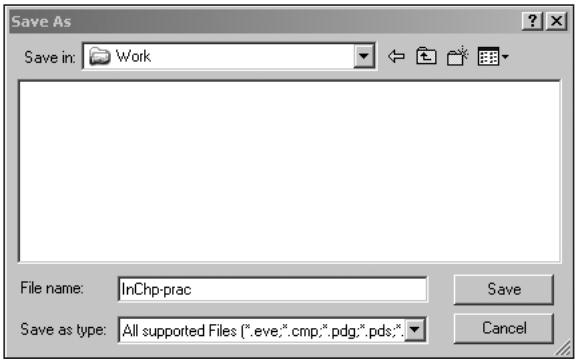


Figure 2-7 The Save As dialog box

6. Next, in the Capture Image dialog box, type your name in the Technician Name text box and **InChp-prac-02** in the Image Number text box (see Figure 2-8). Click **OK**.
7. ProDiscover Basic then acquires an image of the USB thumb drive. When it's finished, it displays a notice to check the log file created during the acquisition. This log file contains additional information if errors were encountered during the data acquisition. ProDiscover also creates an MD5

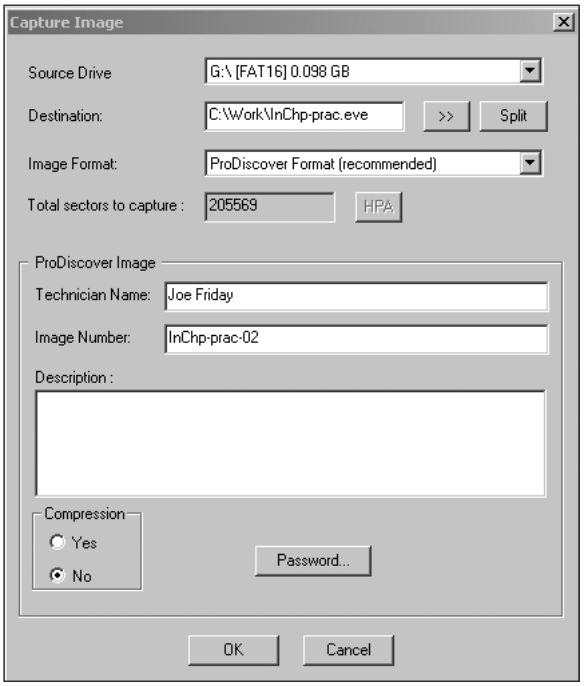


Figure 2-8 The completed Capture Image dialog box

hash output file. In Chapters 4 and 5, you learn how to use MD5 for forensic analysis and evidence validation.

8. When ProDiscover is finished, click **OK** in the completion message box. Click **File**, **Exit** from the menu to exit ProDiscover.

This activity completes your first forensic data acquisition. Next, you learn how to locate data in an acquisition.

Analyzing Your Digital Evidence

When you analyze digital evidence, your job is to recover the data. If users have deleted or overwritten files on a disk, the disk contains deleted files and file fragments in addition to existing files. Remember that as files are deleted, the space they occupied becomes free space—meaning it can be used for new files that are saved or files that expand as data is added to them. The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file. In the meantime, those files can still be retrieved. Forensics tools such as ProDiscover Basic can retrieve deleted files for use as evidence.

In the following steps, you analyze George Montgomery's thumb drive. Before beginning, extract all compressed files from the Chap02 folder on the book's DVD to your work folder. The first step is loading the acquired image into ProDiscover Basic by following these steps:

1. Start ProDiscover Basic, as you did in the previous activity.
2. To create a new case, click **File**, **New Project** from the menu.
3. In the New Project dialog box, type **InChp02** in the Project Number text box and again in the Project File Name text box (see Figure 2-9). Click **OK**.

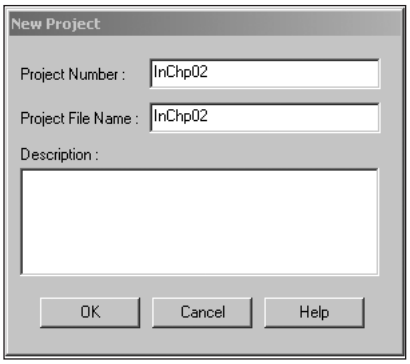


Figure 2-9 The New Project dialog box

4. In the tree view of the main window (see Figure 2-10), click the + (plus symbol) next to the Add item, and then click **Image File**.

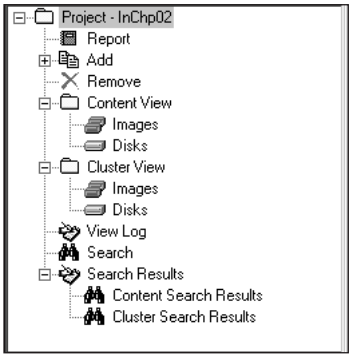


Figure 2-10 The tree view in ProDiscover

5. In the Open dialog box, navigate to the folder containing the image, click the **InChp02.eve** file, and click **Open**. Click **Yes** in the Auto Image Checksum dialog box, if necessary.

The next step is to display the contents of the acquired data. Perform the following steps:

1. In the tree view, click to expand **Content View**, if necessary. Click to expand **Images** and the image filename path **C:\Work\InChp02.eve** (substituting your folder path for "Work"—for example, C:*Work*\Chap02\Chapter).
2. Next, click **All Files** under the image filename path. When the CAUTION dialog box opens, click **Yes**. The InChp02.eve file is then loaded in the main window, as shown in Figure 2-11.

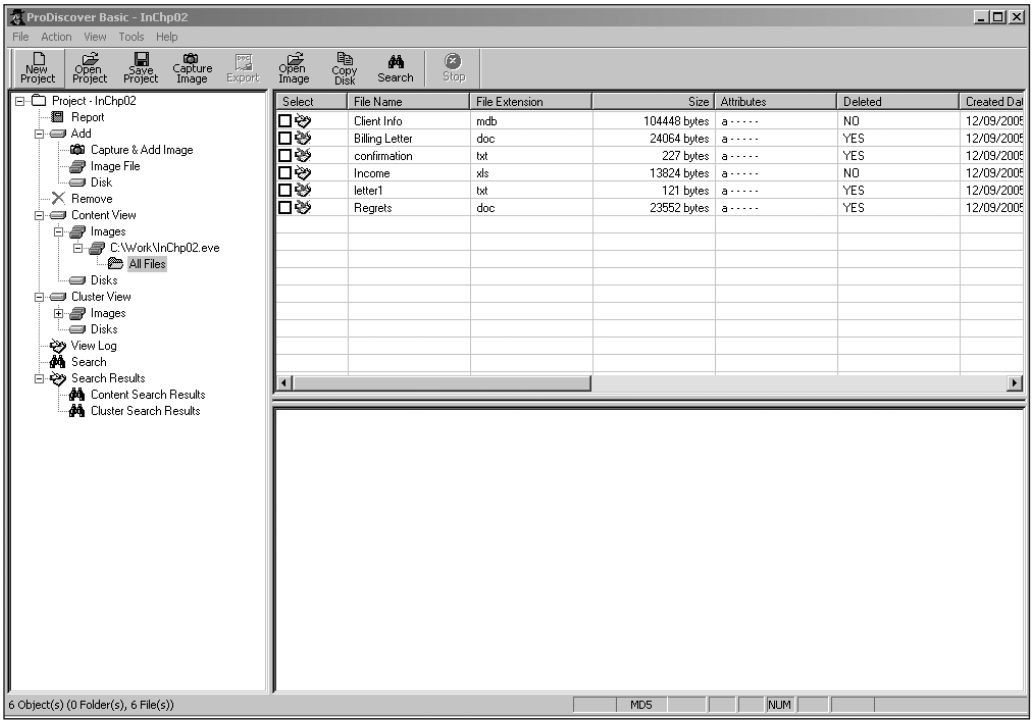


Figure 2-11 The loaded InChp02.eve file

3. In the upper-right pane (the work area), click the **letter1** file to view its content in the data area (see Figure 2-12).
4. In the data area, you see the contents of the letter1 file. Continue to navigate through the work and data areas and inspect the contents of the recovered evidence. Note that many of these files are deleted files that haven't been overwritten. Leave ProDiscover Basic running for the next activity.

The next step is analyzing the data and searching for information related to the complaint. Data analysis can be the most time-consuming task, even when you know exactly what to look for in the evidence. The method for locating evidentiary artifacts is to search for specific known data values. Data values can be unique words or nonprintable characters,

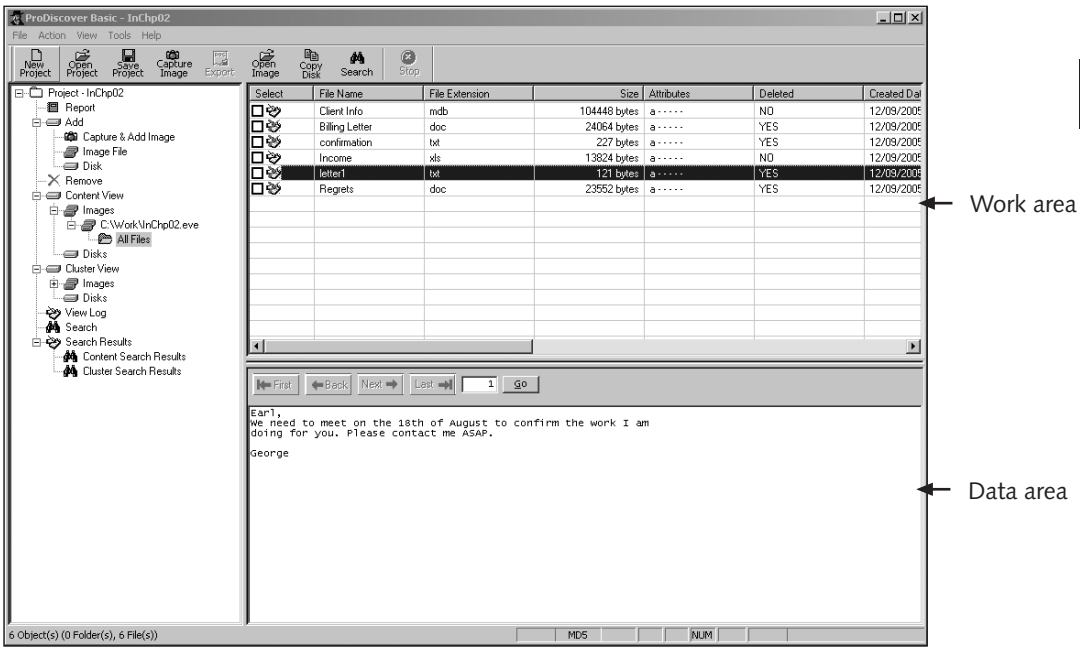


Figure 2-12 Selecting a file in the work area and viewing its contents in the data area

such as hexadecimal codes. There are also unique printable character codes that can't be generated from a keyboard, such as the copyright (©) or registered trademark (™) symbols. Many computer forensics programs can search for character strings (letters and numbers) and hexadecimal values, such as A9 for the copyright symbol or AE for the registered trademark symbol. All these searchable data values are referred to as "keywords."

With ProDiscover Basic, you can search for keywords of interest in the case. For this case, follow these steps to search for any reference to the name George:

1. In the tree view, click **Search**.
2. In the Search dialog box, click the **Content Search** tab, if necessary. Click the **Select all matches** check box, the **ASCII** option button, and the **Search for the pattern(s)** option button, if they aren't already selected.
3. Next, in the text box under the Search for the pattern(s) option button, type **George** (see Figure 2-13).

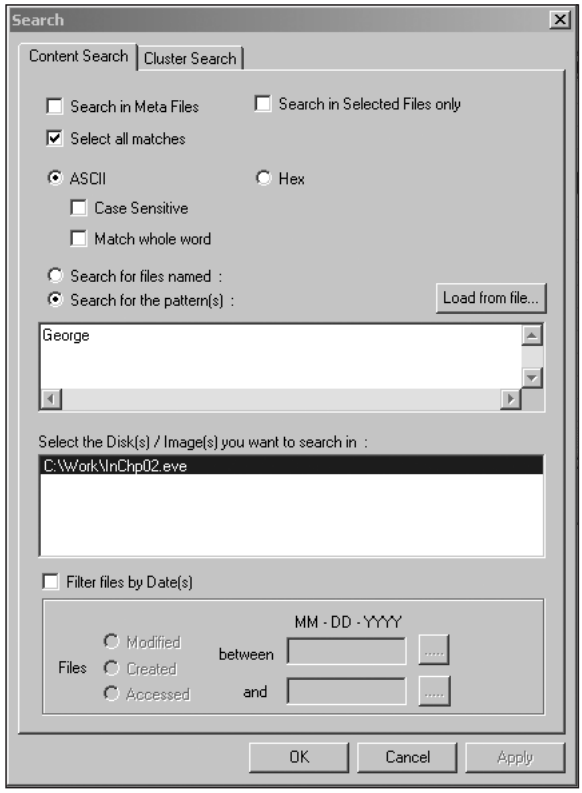


Figure 2-13 Entering a keyword in the Search dialog box

You can list individual keywords or combine words with the Boolean logic operators AND, OR, and NOT. Searching for a common keyword produces too many hits and makes it difficult to locate evidence of interest to the case. Applying Boolean logic can help reduce unrelated excessive hits, which are called "false-positive hits."

4. Under Select the Disk(s)/Image(s) you want to search in, click **C:\Work\InChap02.eve** (substituting the path to your work folder), and then click **OK** to initiate the search. Leave ProDiscover Basic running for the next activity.

When the search is finished, ProDiscover displays the results in a search results window in the work area. Note the tab labeled Search 1 in Figure 2-14. For each search you do in a case, ProDiscover adds a new tab to help catalog your searches.

Click each file in the search results window and examine its content in the data area. If you locate a file of interest that displays binary (nonprintable) data in the data area, you can double-click the file in the search results window to display the data in the work area. Then you can double-click the file in the work area, and an associated program, such as Microsoft

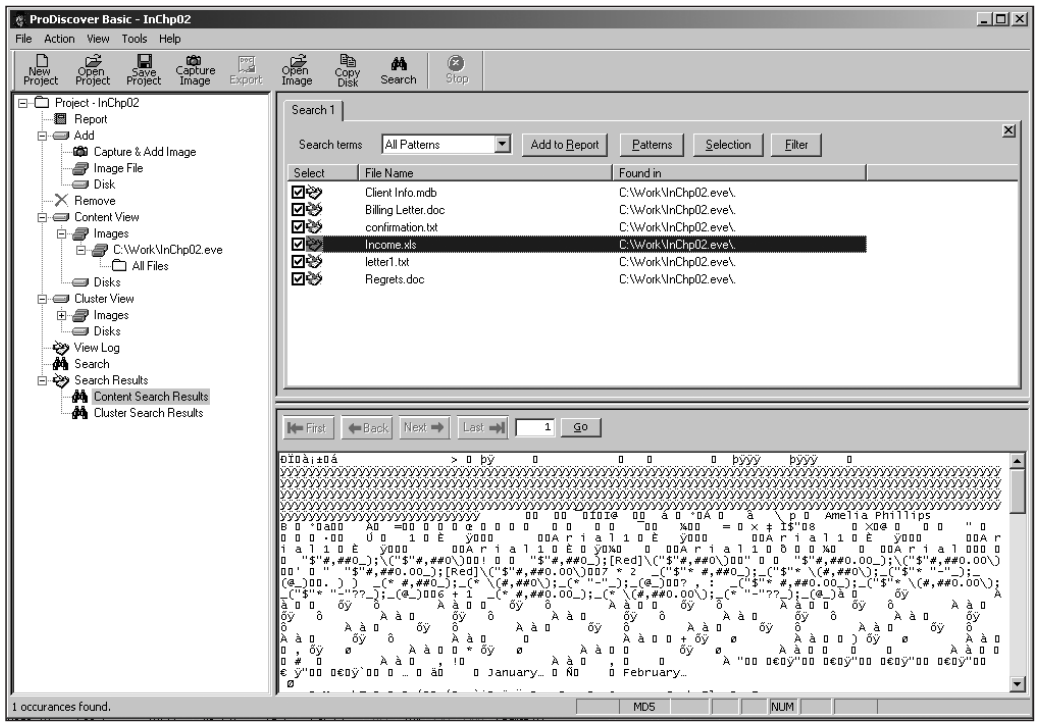


Figure 2-14 The search results window

Excel for a spreadsheet, opens the file's content. If you want to extract the file, you can right-click it and click Copy File from the shortcut menu.

For this example, an Excel spreadsheet named Income.xls is displayed in the search results window. The information in the data area shows mostly unreadable character data. To examine this data, you can export the data to a folder of your choice, and then open it for follow-up examination and analysis. To export the Income.xls file, perform the following steps:

1. In the search results window, double-click the **Income.xls** file, which switches the view to the work area.
2. In the work area, right-click the **Income.xls** file and click **Copy File**.
3. In the Save As dialog box, navigate to the folder you've selected, and click **Save**.
4. Now that the Income.xls file has been copied to a Windows folder, start Excel (or another spreadsheet program, such as OpenOffice Calc) to examine the file's content. Figure 2-15 shows the extracted file open in OpenOffice Calc. Repeat this data examination and file export process for the remaining files in the search results window. Then close all open windows except ProDiscover Basic for the next activity.

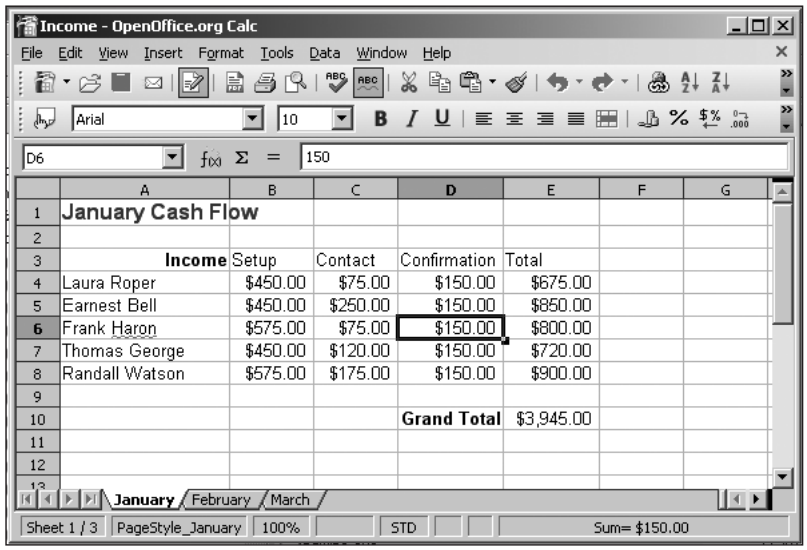

Income - OpenOffice.org Calc
File Edit View Insert Format Tools Data Window Help
Arial
10
D6
150
January Cash Flow
Income Setup Contact Confirmation Total
Laura Roper $450.00 $75.00 $150.00 $675.00
Earnest Bell $450.00 $250.00 $150.00 $850.00
Frank Haron $575.00 $75.00 $150.00 $800.00
Thomas George $450.00 $120.00 $150.00 $720.00
Randall Watson $575.00 $175.00 $150.00 $900.00
Grand Total $3,945.00
January February March
Sheet 1 / 3 PageStyle_January 100% STD Sum= $150.00

Figure 2-15 The extracted Excel file

With ProDiscover's Search feature, you can also search for specific filenames. To use this feature, click the Search for files named option button in the Search dialog box. When you're dealing with a very large disk drive with several thousand files, this useful feature minimizes human error in looking at data.

After completing the detailed examination and analysis, you can then generate a report of your activities. Several computer forensics programs provide a report generator or log file of actions taken during an examination. These reports and logs are typically text files or HTML. The text files are usually in plaintext or Rich Text Format (RTF). ProDiscover Basic offers a report generator that produces an RTF or a plaintext file that can be read by most word processing programs.

You can also select specific items and add them to the report. For example, to select a file in the work area, click the check box in the Select column next to the file to open the Add Comments dialog box. Enter a description and click OK. The descriptive comment is then added to the ProDiscover Basic report. To create a report in ProDiscover Basic, perform the following steps:

1. In the tree view, click **Report**. The report is then displayed in the right pane of the main window, as shown in Figure 2-16.
2. To print the report, click **File**, **Print Report** from the menu.
3. In the Print dialog box, click **OK**.

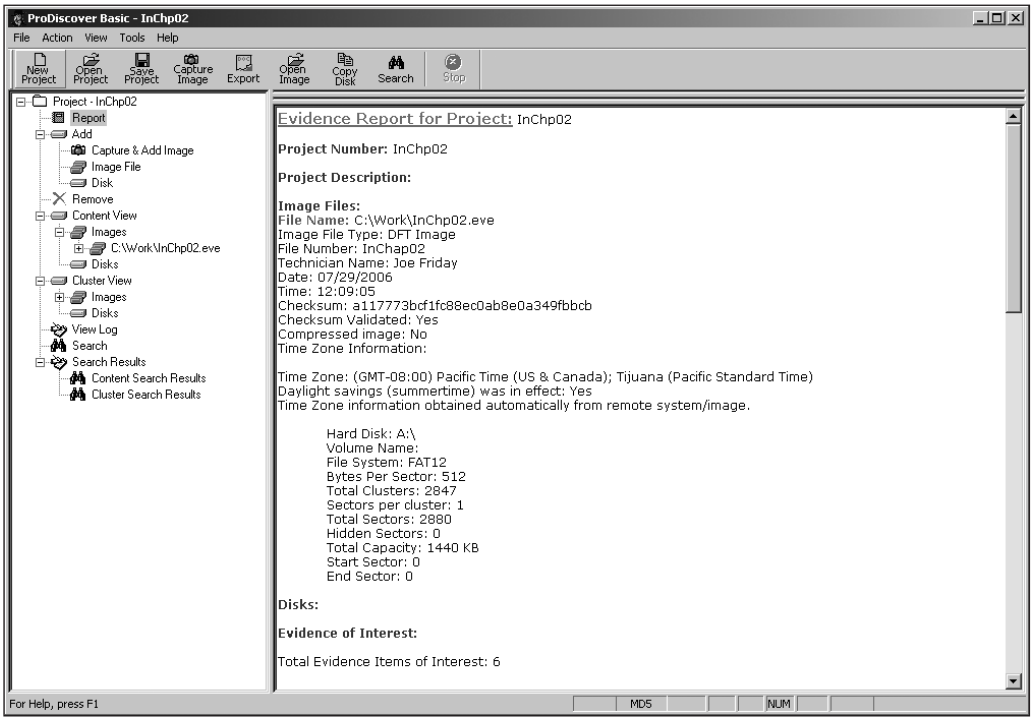


Figure 2-16 A ProDiscover report

If the report needs to be saved to a data file, you use ProDiscover Basic's Export feature and choose RTF or plaintext for the file format. To export the report to a data file, do the following:

1. In the tree view, click **Report**.
2. Now click **Action**, **Export** from the menu.
3. In the Export dialog box, click the **RTF Format** or **Text Format** option button, type **InChp02** in the File Name text box, and then click **OK**.

To place the report in a different folder, click the **Browse** button and navigate to the folder where you want to save the report. Click **Save**, and then click **OK** in the Export dialog box.

4. Review the report, and then click **File**, **Exit** from the menu to exit ProDiscover Basic.

This activity completes your analysis of the USB thumb drive. In the next section, you learn how to complete the case. In later chapters, you learn how to apply more search and analysis techniques.

Completing the Case

After analyzing the disk, you can retrieve deleted files, e-mail, and items that have been purposefully hidden, which you do in Chapters 9, 10, and 12. The files on George's USB thumb drive indicate that he was conducting a side business on his company computer.

Now that you have retrieved and analyzed the evidence, you need to find the answers to the following questions to write the final report:

- How did George's manager acquire the disk?
- Did George perform the work on a laptop, which is his own property? If so, did he perform his business transactions on his break or during his lunch hour?
- At what times of the day was George using the non-work-related files? How did you retrieve that information?
- Which company policies apply?
- Are there any other items that need to be considered?

When you write your report, state what you did and what you found. The report you generated in ProDiscover gives you an account of the steps you took. As part of your final report, depending on guidance from management or legal counsel, include the ProDiscover report file to document your work. In any computing investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as **repeatable findings**; without it, your work product has no value as evidence.

Keep a written journal of everything you do. Your notes can be used in court, so be mindful of what you write or e-mail, even to a fellow investigator. Often these journals start out as handwritten notes, but you can transcribe them to electronic format periodically.

Basic report writing involves answering the six Ws: *w*ho, *w*hat, *w*hen, *w*here, *w*hy, and ho*w*. In addition to these basic facts, you must also explain computer and network processes. Typically, your reader is a senior personnel manager, a lawyer, or occasionally a judge who might have little computer knowledge. Identify your reader and write the report for that person. Provide explanations for processes and how systems and their components work.

Your organization might have templates to use when writing reports. Depending on your organization's needs and requirements, your report must describe the findings from your analysis. The report generated by ProDiscover lists your examination and data recovery findings. Other computer forensics tools generate a log file of all actions taken during your examination and analysis. Integrating a computer forensics log report from these other tools can enhance your final report. When describing the findings, consider writing your narrative first and then placing the log output at the end of the report, with references to it in the main narrative. Chapter 14 covers writing final reports for investigations in more detail.

In the Domain Name case, you would want to show conclusive evidence that George had his own business registering domain names and list the names of his clients and his income from this business. You would also want to show letters he wrote to clients about their accounts. The time and date stamps on the files are during work hours, so you should include that information, too. Eventually, you hand the evidence file to your supervisor or to Steve, George's manager, who then decides on a course of action.

Critiquing the Case

After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and critique the case in an effort to improve your work. Ask yourself assessment questions such as the following:

- How could you improve your performance in the case?
- Did you expect the results you found? Did the case develop in ways you did not expect?
- Was the documentation as thorough as it could have been?
- What feedback has been received from the requesting source?
- Did you discover any new problems? If so, what are they?
- Did you use new techniques during the case or during research?

Make notes to yourself in your journal about techniques or processes that might need to be changed or addressed in future investigations. Then store your journal in a secure place.

Chapter Summary

- Always use a systematic approach to your investigations. Follow the list provided in this chapter as a guideline for your case.
- When planning a case, take into account the nature of the case, instructions from the requester, what additional tools and expertise you might need, and how you will acquire the evidence.
- Criminal cases and corporate-policy violations should be handled in much the same manner to ensure that quality evidence is presented. Both criminal cases and corporate-policy violations can go to court.
- When you begin a case, there might be unanticipated challenges that weren't obvious when applying a systematic approach to your investigation plan. For all investigations, you need to plan for contingencies for any problems you might encounter.
- You should create a standard evidence custody form to track the chain of custody of evidence for your case. There are two types of forms: a multi-evidence form and a single-evidence form.

- Internet and media leak investigations require examining server log data.
- For attorney-client privilege cases, all written communication should have a header label stating that it's privileged communication and a confidential work product.
- A bit-stream copy is a bit-by-bit duplicate of the original disk. You should use the duplicate whenever possible.
- Always maintain a journal to keep notes on exactly what you did when handling evidence.
- You should always critique your own work to determine what improvements you made during each case, what could have been done differently, and how to apply those lessons to future cases.

Key Terms

approved secure container — A fireproof container locked by a key or combination.

attorney-client privilege (ACP) — Communications between an attorney and client about legal matters is protected as confidential communications. The purpose of having confidential communications is to promote honest and open dialogue between an attorney and client. This confidential information must not be shared with unauthorized people.

bit-stream copy — A bit-by-bit duplicate of data on the original storage medium. This process is usually called "acquiring an image" or "making an image."

bit-stream image — The file where the bit-stream copy is stored; usually referred to as an "image," "image save," or "image file."

chain of custody — The route evidence takes from the time the investigator obtains it until the case is closed or goes to court.

computer forensics workstation — A workstation set up to allow copying forensic evidence, whether on a hard drive, thumb drive, CD, or Zip disk. It usually has software preloaded and ready to use.

evidence bags — Nonstatic bags used to transport thumb drives, hard drives, and other computer components.

evidence custody form — A printed form indicating who has signed out and been in physical possession of evidence.

forensic copy — Another name for a bit-stream image.

interrogation — The process of trying to get a suspect to confess to a specific incident or crime.

interview — A conversation conducted to collect information from a witness or suspect about specific facts related to an investigation.

multi-evidence form — An evidence custody form used to list all items associated with a case. *See also* evidence custody form.

password-cracking software — Software used to match the hash patterns of passwords or to simply guess passwords by using common combinations or standard algorithms.

password protected — Requiring a password to limit access to certain files and areas of storage media; this method prevents unintentional or unauthorized use.

repeatable findings — Being able to obtain the same results every time from a computer forensics examination.

single-evidence form — A form that dedicates a page for each item retrieved for a case. It allows investigators to add more detail about exactly what was done to the evidence each time it was taken from the storage locker. *See also* evidence custody form.

Review Questions

1. What are some initial assessments you should make for a computing investigation?
2. What are some ways to determine the resources needed for an investigation?
3. List three items that should be on an evidence custody form.
4. Why should you do a standard risk assessment to prepare for an investigation?
5. You should always prove the allegations made by the person who hired you. True or False?
6. For digital evidence, an evidence bag is typically made of antistatic material. True or False?
7. Who should have access to a secure container?
   a. only the primary investigator
   b. only the investigators in the group
   c. everyone on the floor
   d. only senior-level management
8. For employee termination cases, what types of investigations do you typically encounter?
9. Why should your evidence media be write-protected?
10. List three items that should be in your case report.
11. Why should you critique your case after it's finished?
12. What do you call a list of people who have had physical possession of the evidence?
13. What two tasks is an acquisitions officer responsible for at a crime scene?
14. What are some reasons that an employee might leak information to the press?
15. When might an interview turn into an interrogation?
16. What is the most important point to remember when assigned to work on an attorney-client privilege case?

17. What are the basic guidelines when working on an attorney-client privilege case?
18. Data collected before an attorney issues a memorandum for an attorney-client privilege case is protected under the confidential work product rule. True or False?

Hands-On Projects

In the following Hands-On Projects, continue to work at the workstation you set up in this chapter. Extract compressed files from the Chap02\Projects folder on the book's DVD to your *Work*\Chap02\Projects folder. (If necessary, create this folder on your system to store your files.)

If needed, refer to the directions in this chapter and the ProDiscover user manual, which is in C:\Program Files\Technology Pathways\ProDiscover by default.

Hands-On Project 2-1

The case in this project involves a murder investigation. A USB thumb drive has been seized by the first responding law enforcement officer. A crime scene evidence technician skilled in data acquisition made a bit-stream copy of the thumb drive using ProDiscover and named the bit-stream image C2Prj01.eve. Following the acquisition, she transported and secured the thumb drive and placed it into a secure evidence locker at the police station. You have received the bit-stream copy of the thumb drive from the detective assigned to this case. He directs you to examine and identify any evidentiary artifacts that might relate to this case.

To process this case, locate the **C2Prj01.eve** file you extracted to your work folder. Then start ProDiscover Basic and begin your analysis on this image file to locate any data of interest for the investigation. You need to export any files in this image and present them to the investigator. In addition, write a brief report (no more than two paragraphs) including any facts from the contents of the recovered data.

Hands-On Project 2-2

In this project, you work for a large corporation's IT security company. Your duties include conducting internal computing investigations and forensics examinations on company computing systems. A paralegal from the Law Department, Ms. Jones, asks you to examine a USB thumb drive belonging to an employee who left the company and now works for a competitor. The Law Department is concerned that the former employee might possess sensitive company data. Ms. Jones wants to know whether the thumb drive contains anything significant.

In addition, she informs you that the former employee might have had access to confidential documents because a co-worker saw him accessing his manager's computer on his last day

of work. These confidential documents consist of 24 files with the text "BOOK" in uppercase letters at the beginning of each file. She wants you to locate any occurrences of these files on the thumb drive's bit-stream image.

To process this case, locate the **C2Prj02.eve** file you extracted to your work folder, and load it in ProDiscover. Then analyze it to find occurrences of the keyword "BOOK," using the **Content Search** and **Cluster Search** tabs in the Search dialog box. When you're finished, write a memo to Ms. Jones with the following information: the filename in which you found a hit for the keyword and, if the hit occurred in unallocated space, the cluster number.

Hands-On Project 2-3

Ms. Jones notifies you that the former employee has used an additional disk drive. She asks you to examine this new drive to determine whether it contains an account number the employee might have had access to. The account number, 461562, belongs to the senior vice president and is used to access the company's banking service over the Internet.

To process this case, locate the **C2Prj03.dd** file you extracted to your work folder, and load it in ProDiscover. To aid in your examination, use the **View**, **View Gallery** menu option to examine graphics files, too, for any data related to the account number. Ms. Jones also wants to know whether the disk contains any occurrences of the keyword "BOOK" that you searched for in Hands-On Project 2-2. When you're finished, use the ProDiscover report generator to document the steps you took, and write a memo summarizing your findings.

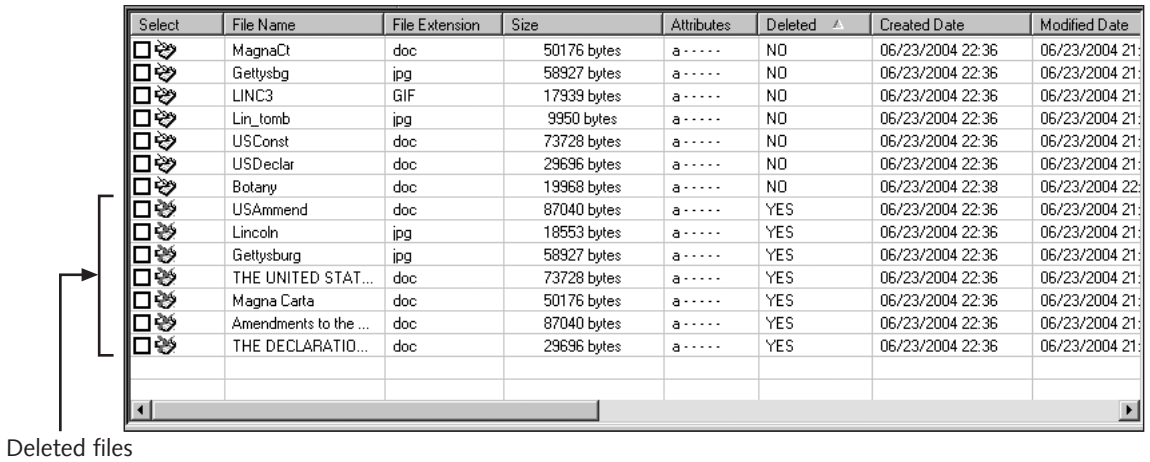
Text can be found in graphics files as well as in documents.

Hands-On Project 2-4

Sometimes discovery demands from law firms require you to recover only allocated data from a disk. This project shows you how to extract just the files that haven't been deleted from an image. Load the **C2Prj04.eve** file you extracted to your work folder into ProDiscover.

The Deleted column in the work area lists YES for deleted files and NO for nondeleted (allocated) files (see Figure 2-17). To make finding nondeleted files easier, you can click the Deleted column header to sort the files into YES and NO groups.

To extract the allocated files from the image to your work folder, right-click each file containing NO in the Delete column and click **Copy File**. (Note that in this tool, there's no way to select multiple files at once. You must copy each allocated file separately.) When you're finished copying all allocated files, save the case by clicking **File**, **Save Project** from the menu.



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date
	MagnaCt	doc	50176 bytes	a-----	NO	06/23/2004 22:36	06/23/2004 21:
	Gettysbg	jpg	58927 bytes	a-----	NO	06/23/2004 22:36	06/23/2004 21:
	LINC3	GIF	17939 bytes	a-----	NO	06/23/2004 22:36	06/23/2004 21:
	Lin_tomb	jpg	9950 bytes	a-----	NO	06/23/2004 22:36	06/23/2004 21:
	USConst	doc	73728 bytes	a-----	NO	06/23/2004 22:36	06/23/2004 21:
	USDeclar	doc	29696 bytes	a-----	NO	06/23/2004 22:36	06/23/2004 21:
	Botany	doc	19968 bytes	a-----	NO	06/23/2004 22:38	06/23/2004 22:
	USAmmend	doc	87040 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:
	Lincoln	jpg	18553 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:
	Gettysburg	jpg	58927 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:
	THE UNITED STAT...	doc	73728 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:
	Magna Carta	doc	50176 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:
	Amendments to the ...	doc	87040 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:
	THE DECLARATIO...	doc	29696 bytes	a-----	YES	06/23/2004 22:36	06/23/2004 21:

Figure 2-17 Deleted files displayed in the work area

Hands-On Project 2-5

This project is a continuation from the previous project; you'll create a report listing all the unallocated (deleted) files ProDiscover finds. In ProDiscover, open the case you saved in Hands-On Project 2-4. Then click the check box in the work area's Select column next to all unallocated files (see Figure 2-18). As you click each check box, the Add Comment dialog box opens, where you can enter a description for the file.

In the Investigator comments text box, add a comment noting that the file is deleted and indicating its file type, such as a Word document or an image file (.jpeg or .gif, for instance).

When you have finished selecting the deleted files, you can print the report for this examination. To do this, click **Report** in the tree view. Next, click **File**, **Print Report** from the menu. After the report is printed, turn it in to your instructor.

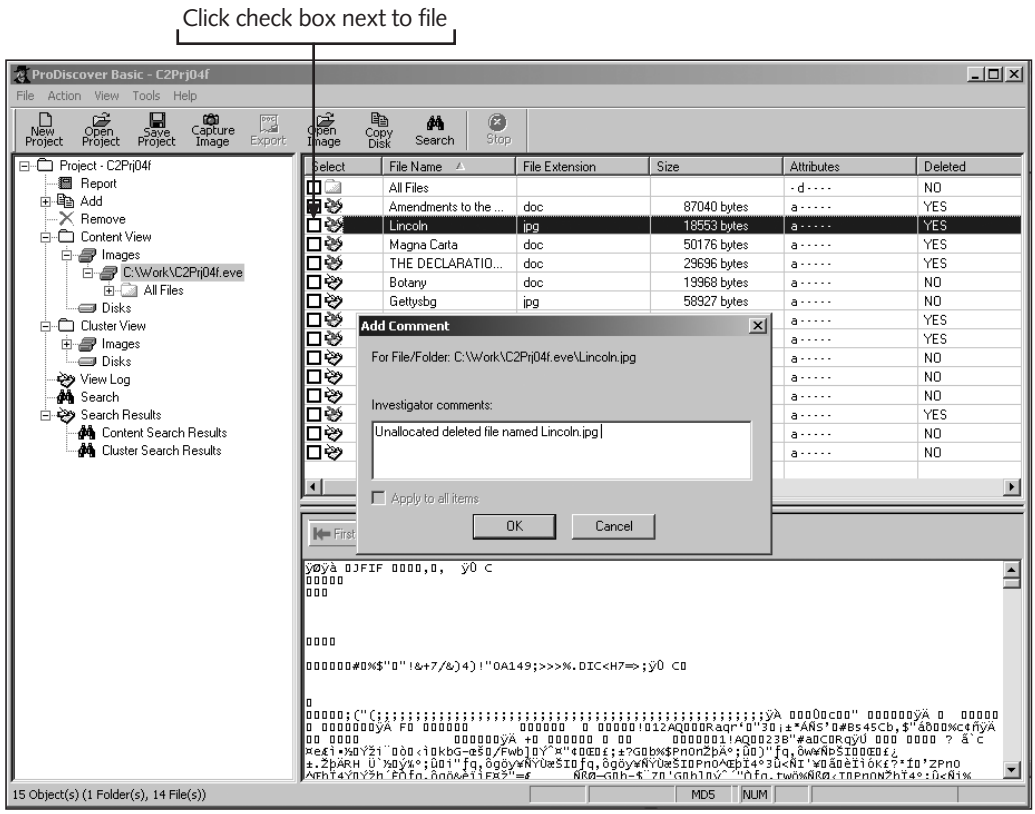


Figure 2-18 Selecting a file to include in a report

Hands-On Project 2-6

In this project, another investigator asks you to examine an image and search for all occurrences of the following words:

- ANTONIO
- HUGH EVANS
- HORATIO

Load the **C2Prj06.eve** file you extracted to your work folder into ProDiscover. When you have located files containing these search words, select them by clicking the check box next to the file in the work area. After you have located all files containing these words, generate a ProDiscover report.

Case Projects

Case Project 2-1

An insurance company has assigned your firm to review a case for an arson investigation. The suspected arsonist has already been arrested, but the insurance company wants to determine whether there's any contributory negligence on the part of the victims. Review the synopsis of the case (refer to the **Firestarter.doc** file you extracted to your work folder), and decide what course of action your firm needs to take. Write an outline for how your firm should approach the case.

Case Project 2-2

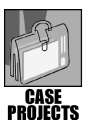
A 14-year-old girl is missing after having an argument with her parents. They call the police at midnight on May 28. A police investigator shows up within 30 minutes to interview them and finds out that the girl spent a lot of time on the Internet. The parents agree to let him take her laptop. What should happen next?

Case Project 2-3

Jonathan Simpson owns a construction company. One day a subcontractor calls him, saying that he needs a replacement check for the job he completed at 1437 West Maple Avenue. Jonathan looks up the job on his accounting program and agrees to reissue the check for $12,750. The subcontractor says that the original check was for only $10,750. Jonathan looks around the office and cannot find the company checkbook or ledger. Only one other person has access to the accounting program. Jonathan calls you to investigate. How would you proceed? Write a one-page report detailing the steps Jonathan needs to take to obtain the necessary evidence and protect his company.

Case Project 2-4

You are the computer forensics investigator for a law firm. The firm acquired a new client, a young woman who was fired from her job for inappropriate files discovered on her computer. She swears she never accessed the files. What questions should you ask and how should you proceed? Write a one- to two-page report describing the computer the client used, who else had access to it, and any other relevant facts that should be investigated.



Case Project 2-5

A desperate employee calls because she has accidentally deleted crucial files from her hard drive and can't retrieve them from the Recycle Bin. What are your options? Write one to two pages that explain your capabilities and list the questions you need to ask her about her system.